UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOES 1–25, *Defendants.*	Civil Action No.: 1:25-cv-04503-JPO

PRELIMINARY INJUNCTION ORDER

Plaintiff Google LLC has filed a Complaint for injunctive and other relief to stop Doe Defendants 1–25 (the "BadBox 2.0 Enterprise") from continuing to control and operate a botnet of over ten million devices (the "BadBox 2.0" botnet), continuing to distribute malware to infect new devices, and continuing to carry out criminal schemes using that botnet.

Google filed a Complaint alleging claims under (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") (Count I) and (2) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)–(d) ("RICO") (Count II). Google has moved under seal and *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not issue under Federal Rule of Civil Procedure 65 and 28 U.S.C. § 1651.

On May 30, 2025, this Court issued a Temporary Restraining Order ("TRO") and order for Defendants to show cause why a preliminary injunction should not issue. On June 6, 2025, this Court extended that TRO until June 27, 2025.

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under the CFAA and RICO pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

a. Defendants distribute malware within this district and New York State.

b. Defendants use that malware to infect user devices in this district.

c. Defendants use that fraudulently installed malware to sell access to the infected user devices so that Defendants and others may use the IP addresses of the infected devices to engage in fraudulent and criminal activity.

d. Defendants send commands to infected user computers in this district and within New York State to carry out their illicit schemes.

e. Google's Complaint and moving papers demonstrate that Defendants undertook these activities intentionally with knowledge that their actions would cause harm to users in New York and cause Google harm in New York. Google does business in New York and has done business in New York for many years.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this district and no other venue appears to be more appropriate.

4. The Complaint pleads facts with the specificity required by the Federal Rules of Civil Procedure and states claims against Defendants for violations of the CFAA, 18 U.S.C. § 1030(a)(4), (a)(5)(A) (Count I) and RICO, 18 U.S.C. § 1962(c)–(d) (Count II).

Preliminary Injunction Order Factors

5. The Court finds that Google has established each of the factors required for a preliminary injunction: (1) irreparable harm; (2) a likelihood of success on the merits and/or has established a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a preliminary injunction serves the public interest. *Benihana, Inc. v. Benihana of Tokyo, LLC,* 784 F.3d 887, 895 (2d Cir. 2015); *see also Sterling v. Deutsche Bank Nat'l Tr. Co. as Trustees for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019) ("The standard[s] for granting a temporary restraining order and a preliminary injunction pursuant to Rule 65 of the Federal Rules of [Civil] Procedure are identical.").

Irreparable Harm

6. Google has established that it will suffer immediate, irreparable harm if this Court denies its request for a preliminary injunction. Google has shown that Defendants—through their participation in, and operation of, the BadBox 2.0 Enterprise—have threatened the security of the internet, including Google platforms, by transmitting malware through the internet to configure, deploy, and operate a botnet. Defendants have distributed malware on user devices that use the Android Open Source Project ("AOSP") operating system, which Google created and retains a role in overseeing, that compromises the security of those devices, exploits those devices to carry out a variety of advertising frauds, including through the Google Ad Network, and makes those devices tools of various other cybercrimes by selling access to those devices to other threat actors so that they may connect to an infected device's IP address and use it to mask their location.

7. The Defendants control a botnet that has infected more than ten million devices. At any moment, the botnet could be harnessed for additional criminal schemes. Defendants could, for example, enable large ransomware or distributed denial-of-service attacks on legitimate businesses and other targets. Defendants could themselves perpetrate such a harmful attack, or they could sell access to the botnet to a third party for that purpose.

8. In addition, Defendants' conduct is injuring Google's goodwill and damaging its reputation by falsely associating Google and the Android operating system with the fraud perpetrated by the BadBox 2.0 botnet. Google has suffered and continues to suffer economic losses from Defendants' ad fraud on the Google Ad Network. In addition, Google has expended (and continues to expend) substantial financial resources to investigate the BadBox 2.0 botnet and to identify measures necessary to remediate the harms caused by the botnet. These injuries constitute irreparable harm, including because Google has shown a likelihood that Defendants would not comply with a judgment for money damages.

Likelihood of Success on the Merits

9. Google has shown not only that its Complaint presents a substantial question as to each of its claims but that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trs. for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

10. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the CFAA. The CFAA prohibits, among other things, knowingly causing the transmission of a program, information, code, or command to a protected computer and as a result intentionally causing damage without authorization. 18 U.S.C. § 1030(a)(5)(A). And the CFAA prohibits accessing a protected computer without authorization (or in excess of authorization) knowingly and with intent to defraud when such

access furthers the intended fraud and enables the perpetrator to obtain something of value. *Id.* § 1030(a)(4). Defendants violated both provisions, infecting over ten million devices worldwide and tens of thousands of devices in the Southern District of New York alone. Defendants did so by intentionally causing malware and commands to be transmitted to infected devices, which are used in or affect interstate or foreign commerce or communication, without users' knowledge or consent and doing so to further Defendants' fraudulent schemes, resulting in considerable value to Defendants. Defendants' actions have caused loss to Google in excess of $5,000 in a one-year period.

11. *RICO*. Google has shown a likelihood of success on the merits of its claim that Defendants have violated and continue to violate the RICO statute.

a. Google has shown that Defendants are active participants in the operation and management of the BadBox 2.0 botnet, which is connected to "command-and-control" servers ("C2 Servers") associated with perpetrating fraudulent ads and proxying activity on infected devices. The Infrastructure Group established and manages the C2 infrastructure (C2 Servers and domains) for BadBox 2.0. The Backdoor Malware Group developed and preinstalls malware on the BadBox 2.0 devices and uses that malware to operate a botnet composed of a subset of BadBox 2.0-infected devices and to carry out a variety of ad fraud campaigns. The Evil Twin Group develops apps that the BadBox 2.0 Enterprise uses to commit ad fraud via hidden ads. The Ad Games Group is connected to an ad fraud campaign conducted through BadBox 2.0-infected devices that uses fraudulent "games" to generate ads in hidden web browsers.

b. Google has established that Defendants constitute an enterprise. Defendants share a common purpose to spread malware to build a botnet that is deployed for numerous criminal schemes for profit. Defendants work together to accomplish this purpose, each playing a role as described above, using a shared infrastructure, and collaborating to fulfill their common purpose.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the CFAA, *id.* § 1030(a)(5)(A). Defendants have violated and continue to violate the CFAA, *id.*, resulting in damage as defined in § 1030(c)(4)(A)(i)(VI), by infecting protected computers with malware designed to carry out their schemes. The predicate acts also include violations of the federal wire fraud statute, 18 U.S.C. § 1343, which Defendants have violated and continue to violate by transmitting signals in interstate or foreign commerce for the purpose of executing their various fraudulent schemes.

d. Google has suffered injury to its business or property as a result of these predicate offenses, including through Defendants' ad fraud schemes and use of the botnet to sell residential proxy access, by the refunds Google issues for fraudulent ad traffic, and by devoting substantial financial resources to investigate and combat Defendants' criminal schemes in order to protect its goodwill and reputation.

Balance of Hardships

12. The equities also favor a preliminary injunction. The BadBox 2.0 Enterprise is defrauding consumers and injuring Google, and the BadBox 2.0 botnet is growing in size and capability. No countervailing factors weigh against a preliminary injunction. There is no legitimate

reason why Defendants should be permitted to continue to disseminate malware and manipulate infected devices to carry out criminal schemes.

Public Interest

13. Google has shown that the public interest favors granting a preliminary injunction.

14. Every day that passes, Defendants infect new devices, engage in more fraud, facilitate other threat actors' cybercrimes by selling access to the IP addresses of infected devices, and deceive more unsuspecting victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

15. The public interest is clearly served by enforcing statutes designed to protect the public, including the CFAA and RICO.

Good Cause for Alternative Service

16. The Court finds good cause exists to grant alternative service of the filings in this matter via email using any information available from web-hosting companies provided in connection with domain names used in the BadBox 2.0 botnet and/or any email addresses identified through Google's investigation; website publication; and/or other means because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, online alternative service is most likely to give Defendants notice of the filings pertaining to this lawsuit. Google will send notice by ordinary mail to the extent an address is available.

PRELIMINARY INJUNCTION ORDER

IT IS HEREBY ORDERED that Defendants, any of their officers, agents, servants, employees, or attorneys, and all others in active concert or participation with them, who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are preliminarily restrained and enjoined, from, anywhere in the world:

1. Intentionally accessing and sending malicious code to the protected computers of Google's customers without authorization;

2. Sending malicious code to configure, deploy, and operate a botnet;

3. Attacking and compromising the security of the devices and networks of Google's customers, including through modified versions of AOSP;

4. Stealing and exfiltrating information from computers and computer networks;

5. Configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in Google's moving papers, including but not limited to (i) the C2 Servers operating through the domains listed in Appendix A to the Complaint; (ii) the domains being monetized by Defendants listed in Appendix A to the Complaint; and (iii) through any other component or element of the botnet in any location;

6. Delivering malicious code designed to provide proxy access in order to take over the device or engage in ad fraud;

7. Engaging in the sale of proxy services as described in the moving papers;

8. Engaging in ad fraud as described in the moving papers;

9. Using, linking to, transferring, selling, exercising control over, or otherwise owning or accessing the domains attached in Appendix A; and/or

10. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

11. Upon service as provided for in this Order, Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Order, and any act by any of the Restrained Parties in violation of any of the terms of the Order may be considered and prosecuted as contempt of court.

12. In the event Google identifies additional domains or entities used in connection with or participating in Defendants' scheme, Google may move the Court for an order modifying this Order as appropriate and may amend its Complaint to include the additional parties.

IT IS FURTHER ORDERED that Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in Appendix A, requesting that those persons and entities take best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

2. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

3. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move their botnet infrastructure, as identified by Google in any supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet or continue to perpetrate illegal acts;

4. Disable completely the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

5. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

6. Transfer any content and software hosted at the domains listed in Appendix A that are not associated with Defendants, if any, to new domains not listed in Appendix A; notify any non-party owners of such action and the new domains, and direct them to contact Google's counsel Laura Harris at King & Spalding LLP, 1185 Avenue of the Americas, 34th Floor, New York, New York 10036-2601, and lharris@kslaw.com, to facilitate any follow-on action;

7. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

8. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

9. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

10. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

11. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

12. In determining the method and mechanism to disable content and software associated with Defendants, the relevant persons and/or entities shall reasonably confer with Plaintiff's counsel of record in this action.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, with respect to any currently registered Internet domain set forth in Appendix A, the domain registries shall take or cause to be taken the following actions:

1. Within three (3) business days of receipt of this Order, or as soon as practicable, unlock and change the registrar of record for the domain or such other registrar specified by Google. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, or as soon as reasonably practicable, shall change, or assist in changing, the registrar of record for the domain or such other registrar specified by Google. The purpose of this paragraph is to ensure that Google has control over the hosting and administration of the domain in the registrar account specified by Google. Google shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

2. The domains shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Google, upon taking control of the domains;

3. Take reasonable steps to work with Google to ensure the transfer of the domains and to ensure that Defendants cannot use the domains to obtain unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them, or engage in any other activities prohibited by this Order;

4. The WHOIS registrant, administrative, billing, and technical contact and identifying information should provide such information as may be specified by Google;

5. Prevent transfer, modification, or deletion of the domains by Defendants and prevent transfer or control of the domain to the account of any party other than Google;

6. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that Google may seek leave of Court to amend Appendix A to the Complaint if it identifies other domains or IP addresses used by Defendants in connection with the BadBox 2.0 Enterprise.

Security for Preliminary Injunction Order

IT IS FURTHER ORDERED that Google's submission of the $75,000 bond to the Clerk satisfied the requirements of this Court's TRO. No additional bond is necessary.

So ordered.

June 27, 2025
New York, New York

J. PAUL OETKEN
United States District Judge